

ROUTING AND TRANSMITTAL SLIP

Date

27 MAR 86

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. EXO/DDA	<i>[Signature]</i>	27.3
2. ADDA	<i>[Signature]</i>	
3. DDA	<i>[Signature]</i>	3/27
4. DDA PLANS	<i>[Signature]</i>	3/28
5. DDA REC.	<i>[Signature]</i>	3/31

Action	File	Note and Return
Approval	For Clearance	Per Conversation
As Requested	For Correction	Prepare Reply
Circulate	For Your Information	See Me
Comment	Investigate	Signature
Coordination	Justify	

REMARKS

D/OS RECEIVED A COPY.

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, org. symbol, Agency/Post)

Room No.—Bldg.

Phone No.

5041-102

* U.S.G.P.O.: 1983-421-529/320

OPTIONAL FORM 41 (Rev. 7-76)
Prescribed by GSA
FPMR (41 CFR) 101-11.206

EXECUTIVE SECRETARIAT ROUTING SLIP

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI				
3	EXDIR		X		
4	D/ICS				
5	DDI		X		
6	DDA		X		
7	DDO		X		
8	DDS&T		X		
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/OLL				
14	D/PAO				
15	D/PERS				
16	VC/NIC				
17	D/Security		X		
18	C/CI/DO		X		
19	NIO/FDIA		X		
20	C/Security Comte		X		
21					
22					
		SUSPENSE _____ Date			

Remarks

[Signature] Executive Secretary
26 Mar 86
Date

3637 (10-81)

25X1

SECRET
The Director of Central Intelligence
Washington, D.C. 20505

D/ICS-86-0794
24 March 1986



The Honorable Dave Durenberger, Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510



25X1

Dear Dave:

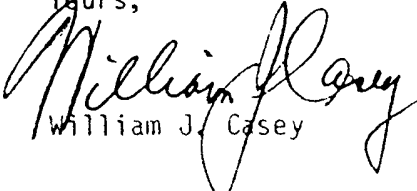
Last month, I provided Chairman Hamilton and you a statement of our progress in developing the Presidential report mandated by Section 402 of the Intelligence Authorization Act for FY 1986. By mutual agreement, that interim response included extensive comments on the counterintelligence section of the draft report on Espionage and Security that your Committee is preparing for the Senate. Those comments were intended to be constructive and to assist in shaping your Committee's report. Dick Stilwell informs me that they have indeed proved helpful and that, as a result of follow-on staff discussions, substantive agreement has been reached on all but one of the numerous recommendations in that portion of the draft report.

We have addressed the draft of the Countermeasures section in the same spirit. Stilwell's working group was again assigned responsibility for review and developed comments on the 52 recommendations. The SIG-I considered the working group's report last week and, as before, concluded that it constituted a sound basis for fruitful dialogue with your Committee. I hope you will find the comments equally helpful.

Your Staff is to be complimented for what the SIG-I knows full well has been a difficult undertaking in brigading the several interrelated security disciplines. It is more complex than the counterintelligence area in both structure and content. Staff consultations will thus be particularly important to our effort to reach mutual understanding. For example, I call your attention to the final paragraph of the first comment, which I personally endorse.

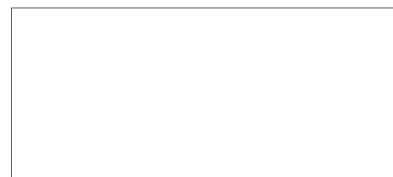
I look forward to discussing these matters with the Committee at the forthcoming hearings.

Yours,


William J. Casey

Enclosure

Regrade Unclassified upon removal
of classified enclosure



25X1

SECRET

CCIS/ICS [redacted] (24 March 1986)

STAT

Distribution (all w/encs) (D/ICS-86-0794):

- 0 - Addee
- 1 - DCI
- 1 - DDCI
- 1 - ES
- 1 - ER
- 1 - D/ICS
- 1 - DD/ICS
- 1 - LL/ICS
- 1 - PBS/ICS [redacted]
- 1 - SIG-I Secretariat [redacted]
- 1 - ICS Registry
- 1 - CCIS/ICS subject
- 10 - SIG-I Secretariat (for distribution to SIG-I principals)
(letter only -- CCIS chrono)

STAT

STAT

SECRET
The Director of Central Intelligence
Washington, D.C. 20505

D/ICS-86-0795
24 March 1986

The Honorable Lee H. Hamilton, Chairman
Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

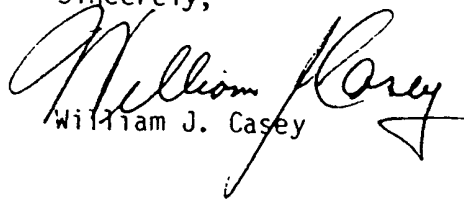
Dear Mr. Chairman:

On 12 February, I provided Chairman Durenberger and you a mid-point statement of progress on the development of the Presidential report, mandated in the Intelligence Authorization Act for FY 1986, on plans to enhance the national counterintelligence and security posture. That interim response included, at the request of your counterpart Committee, comments on the counterintelligence section of the report on Espionage and Security that the SSCI is preparing for the Senate.

We subsequently received the draft of the Countermeasures (security) portion of the SSCI report and have followed the same procedure for subjecting it to critical review. Specifically, General Stilwell's working group developed comments on the 52 recommendations. The SIG-I then met on this matter and concluded that, while the comments have no official status, they constitute a sound basis for continuing dialogue with the SSCI Staff.

I attach a copy of the comments which I am simultaneously transmitting to Chairman Durenberger.

Sincerely,


William J. Casey

Enclosure

Regrade Unclassified upon removal
of classified enclosure

SECRET



25X1

SECRET

1. The Executive Branch should develop and implement a comprehensive National Strategic Security Program to provide policy direction and coordination for all security disciplines. A single body should be assigned to assist the NSC for this purpose, with adequate staff support; and a senior official should be designated to testify on the program before the appropriate Congressional committees. The essential features of the program should be promulgated by the President in an executive order to provide long-term stability.

COMMENT: Attention is invited to the commentary previously provided to the Committee on the first two recommendations in the Counterintelligence section of the SSCI draft. That commentary is generally applicable to the above recommendation.

Thus, the key features of a sound posture, in both CI and CM areas are:

- NSC-approved objectives and derivative policies;
- a broad master plan faithful to the objectives/policies and informed and prioritized by the threat;
- close coordination of implementing programs which are interagency by their very nature and decentralized execution of those that are not;
- continuous interagency exchange of all relevant information and full cooperation in research and training;
- mechanisms for periodic overall review and evaluation at the national level;
- strengthened oversight at all levels; and
- adequate resourcing.

Some of these features are structural and, for the most part, already in place. Some are programmatic, within the purview of department and agency heads and sensitive to annual budget determinations. And some--probably the most important--involve the ability of the various entities of the security community to forge optimum working relations.

SECRET

SECRET

This entire matter will be addressed in the President's report. However, it is clear that the totality of a national counterintelligence/security system cannot be set forth in any single document--labelled National Strategic Security Program or other--and that no single official can speak for all security disciplines and all interagency bodies, or agencies which perform interagency functions in this area. By consequence, the comments hereinafter deal only with the substance of SSCI recommendations, reserving with respect to the vehicle or vehicles by which promulgated and implemented.

2. The Defense Department should enhance its security policy and oversight capabilities in OSD so as to ensure integration of policies for the various DoD security programs.

COMMENT: Concur. DoD is now staffing relevant recommendations of the Stilwell Commission.

3. The National Strategic Security Program should evaluate security countermeasures resource priorities for the NSC and OMB on an annual basis. Security resources should be identified by function and program in departmental and agency budget justifications. The Administration and the Congress should consider additional ways to implement a more coherent budget process for security programs.

COMMENT: See comment on Recommendation 1.

Concur with the final sentence. As to balance of recommendation:

- Not all resources devoted to security can be separately identified. However, it should be noted that a national-level program already exists for the review and assessment of the telecommunications and automated information systems security programs and budgets for the US Government.
- Department/agency heads, charged as they are with the safeguarding of information and other property entrusted to their care, must determine the appropriate mix of security measures within the resources made available by Congress.

SECRET

SECRET

- Periodic evaluation of priorities, executive branch-wide, would not be particularly meaningful. On the other hand, such evaluations might be helpful in illuminating major differences in approach among departments/agencies, areas where putative vulnerability rather than threat has been criterion for resource allocation and uneven support of joint programs.

4. The National Strategic Security Program should assess requirements for research and analysis on security countermeasures to promote aggressive and balanced efforts government-wide, especially on personnel security.

COMMENT: Concur. Comparable recommendations of Stilwell Commission have been endorsed by the IG/CM.

5. The National Strategic Security Program should emphasize commander and manager responsibility for security, including government-wide application of the recent DoD action to incorporate security into performance evaluations and develop more realistic and consistent policies for disciplinary sanctions.

RESPONSE: Concur.

6. The National Strategic Security Program should commission an independent evaluation of the recruitment, training, pay, status, professional development, and retention of federal security personnel. Relevant OPM job classifications should be revised and modernized.

COMMENT: Concur that the executive branch should undertake an overall evaluation. Department of Defense has requested OPM to revise the Classification Standard for Security (080), and Department of State has key actions under way in this general area.

7. The National Strategic Security Program should establish government-wide security training objectives and should require minimum levels of training and certification for industrial security officers, clearance adjudicators, and other positions requiring consistent standards.

COMMENT: Concur.

SECRET

8. The National Strategic Security Program should consider assignment of national responsibilities for security training to the Defense Security Institute, with an interagency group including representation from US counterintelligence agencies to develop security awareness materials and with a West Coast annex.

COMMENT: Five or more years will elapse before the Defense Security Institute (DSI) is organized, staffed, and otherwise prepared to shoulder the full range of tasks recently levied by the SecDef. Consequently, it will not be feasible for DSI to assume interagency training responsibilities for the foreseeable future except on a case-by-case basis. The concept of interagency collaboration in the development and exchange of security awareness material is endorsed.

9. The National Strategic Security Program should develop government-wide operations security (OPSEC) objectives and ensure that the relevant agencies have the necessary resources and programs to achieve those goals.

COMMENT: Concur with development of OPSEC objectives; a draft NSDD is now being coordinated.

OPSEC plans and measures are essentially non-programmatic. Therefore, there are not now--nor should there be--department and agency resources specifically allocated for this function.

10. The National Strategic Security Program should ensure substantially increased funding for personnel security in all relevant departments and agencies. A Government-wide plan should be submitted to Congress to achieve the following goals: (a) elimination of the reinvestigation backlog for Top Secret (including SCI) within four years; and (b) implementation within less than ten years of a program for intensified investigation and reinvestigation for Secret clearances.

SECRET

COMMENT: These are reasonable goals and, in fact, have already been adopted by DoD, which has 90 percent of the cleared population. However, the reinvestigation targets should not be pursued in a vacuum; it is at least as important to invest in personnel research to improve the quality of investigations, to establish better controls over the number of clearances, to develop more rigorous and uniform adjudication standards, and to engage supervisors in the continuing appraisal of subordinates from a security standpoint.

Standards for initial investigations are being developed by the DoJ-led working group mandated by NSDD-84.

11. Agreement should be reached as soon as possible on a "single scope" background investigation for all Top Secret and SCI clearances. The uniform policy should provide for: (a) less costly and more timely background investigations and clearances; (b) highest priority for meeting the five-year reinvestigation requirement; and (c) a subject interview in all cases.

COMMENT: The above referenced working group is charged with recommending a government-wide standard for Top Secret clearances. The DCI has statutory responsibilities for SCI clearance standards. While there is merit in identical Top Secret and SCI standards--and DoD has repeatedly so urged--it is not an achievable result unless and until the personnel research effort DoD has under way leads to major change in the methodology for determining an individual's bona fides.

Concur in principle that reinvestigations should have higher priority than accorded in recent years. However, the caveats expressed in the comment on Recommendation 10 apply.

12. Government-wide minimum standards should be established for the use of contractors for background investigations, including requirements for supervision and quality control, restrictions on use of information, exclusion of contractors from adjudication, and standards for experimentation with new procedures for less sensitive clearances.

COMMENT: No objection to basic rules to govern the "contracting out" of background investigations. However, the detailed modalities need further study and must be adapted to the unique policies of the departments and agencies concerned.

SECRET

SECRET

13. A new reliability clearance program should be established for persons needing access to sensitive sites, but not access to classified information maintained there. Standards for a reliability clearance must be at least as stringent as the proposed standards for a Secret clearance.

COMMENT: Delete. This is an area where commonality is neither desirable nor practical. Even within DoD, components determine their own standards for facility-only access, totally outside the security clearance program.

14. More effective means should be established for investigating and clearing immigrant aliens and foreign nationals granted access to classified information.

COMMENT: Concur in principle. However, the only practical method is to adopt, as DoD has done, extended US residency requirements as well as CI-scope polygraph examinations when access is to be granted at the Secret level.

15. Implementation of the proposal for one-time, short-duration access by cleared personnel to the next highest level of classified information should be postponed until Secret clearance requirements and investigations are upgraded.

COMMENT: The Secretary of Defense has already approved the related recommendation of the Stilwell Commission, and a directive establishing rigid controls is now being coordinated with DoD components. Extent and manner of utilization of this authority will be monitored and evaluated, and results shared with the IG/CM members. It is to be noted that this special authority does not extend to the category of SCI.

16. The Executive branch should consider requiring persons with Top Secret clearances to furnish financial data in background investigations and to consent to access to relevant financial records for such purposes and for a period of time after clearance terminates. Congress should consider legislation to require financial institutions to provide such access.

COMMENT: Concur in principle with the requirement for financial disclosure. Enforcement on a selective basis has clear merit. Application across the board has implications which need further study.

SECRET

17. The National Strategic Security Program should increase personnel security research, including expanded research and evaluation on the wider use of psychological testing and in the clearance process, taking full account of the individual rights, as well as the implications of recent espionage cases.

COMMENT: Concur.

18. The President should issue a new executive order on personnel security. The order should provide for government-wide minimum standards and procedures and a policy oversight office similar to the Information Security Oversight Office. It should focus exclusively on personnel security programs regarding access to classified information and to sites where classified information is maintained. Drafting of this order should not delay action on other recommendations.

COMMENT: The DoJ-led working group, mandated by NSDD-84, has these matters under active consideration, and is charged to provide recommendations to the NSC.

19. The National Strategic Security Program should improve the adjudication process for granting or denying security clearances, with more rigorous standards regarding persons who have committed felony offenses; follow-up inquiries where persons with admitted problems like drug use are cleared; and a government-wide requirement for training of adjudicators. For the most sensitive positions, a "select in" policy based on demonstrated aptitude for security should be adopted in place of the current "select out" policy based on the absence of proven disqualifications.

COMMENT: Concur with the need to improve the adjudication process, particularly regarding qualification standards for adjudicators and more rigorous and consistent criteria for clearance denial.

SECRET

A "select in" policy is an intriguing concept. However, it needs further study to determine feasibility of implementation in a consistent and equitable manner.

20. The National Strategic Security Program should ensure full coordination of departmental policies and practices for the use of polygraphing in personnel security screening, to maintain stringent quality controls and safeguards for individual rights, to prevent overreliance on this techniques, to provide for necessary research and funding, to upgrade the national training center, and to improve understanding of the procedures.

COMMENT: Concur but with a reservation and a clarification:

- The policies and practices in effect in CIA and NSA for the use of polygraph examinations in personnel security screening are very different from the limited use for this purpose within the other components of DoD. Thus, "coordination"--for which purpose an interagency forum now exists--should not be construed to imply as modifying the relevant policies of the three parties concerned.
- There is no national training center nor is one contemplated. The DoD Polygraph Institute provides training for a number of non-DoD departments and agencies. Since 1952, the CIA has had an in-house capability, geared to meeting its unique needs. This arrangement is eminently satisfactory.

21. Congress should consider permanent legislation authorizing DoD to use polygraph examination for personnel security screening with CI-related questions, based on the most recent DoD proposal. Congress should require adequate DoD policy oversight and inspection to ensure consistent implementation and quality control, with the SEVEN SCREENS program as a possible model.

COMMENT: Concur.

22. The other Stilwell Commission recommendations on personnel security should be implemented vigorously in DoD with augmented OSD policy oversight, and they should be reviewed at the NSC level for adoption government-wide.

SECRET

SECRET

COMMENT: The Secretary of Defense has directed implementation of the referenced recommendations, and they are under review by the IG/CM to determine which should be proposed to the NSC for adoption throughout the executive branch.

23. Immediately implement the ISOO proposals with strong public endorsement of the President and the principal members of the National Security Council.

COMMENT: The 13 proposals, developed by an interagency group under the aegis of the Director, ISOO, are under active review at the NSC level. It is anticipated that decision thereon will be reflected in the President's final report.

24. Consider simplifying the classification system by establishing two levels, eliminating the current Confidential classification.

COMMENT: Disagree. The reasons for retaining the Confidential classification are overwhelming. Two statistics are pertinent:

- Seventy-seven percent of the enormous DoD holdings are at the Confidential level. The cost of upgrading to Secret in terms of physical security, accountability requirements, and degradation of tactical mobility would be staggering.
- Hundreds of arrangements with other countries would be disrupted and require renegotiation. Sweden excepted, all these countries have a three- or four-tier security classification system.

25. By executive order, require each agency to establish procedures governing authorized disclosure of classified information to the news media, including background disclosures of information that remains classified. Such procedures should require records for accountability, consultation with originating agencies, and designation of officials authorized to disclose classified information to the media.

COMMENT: Concur with intent. This important subject, basic to the control of leaks, was specifically addressed in NSDD-84. Implementing procedures--to include designation of officials authorized to make disclosures and under what conditions--are under review.

SECRET

SECRET

26. Modify Executive Order 12356 to place more controls on special access programs and to give the ISOO Director greater authority to oversee such programs. Conduct a comprehensive, one-time review and revalidation of all existing special access programs and associated "carve out" contracts, with an independent assessment by the ISOO Director.

COMMENT: Do not believe that Executive Order 12356 needs to be more specific as to controls imposed on special access programs. Section 4.2 thereof adequately defines the rules and charges agency heads themselves with compliance. Problems in the past have resulted from less than full enforcement of the rules. In this connection, the Secretary of Defense, responsible for the greatest number of special access programs, has recently directed several actions to strengthen validation control and oversight. These include an annual review which is appropriate for other departments and agencies.

One change in Executive Order 12356 under consideration is to facilitate the Director, ISOO's discharge of his responsibility by allowing him to delegate his now exclusive authority for access to agency systems of accounting.

27. Expand ISOO's staff to include a permanent inspection element. ISOO should work with DIS to implement improved training courses on information security and classification management. ISOO and the DCI should also reassess special markings with a view to simplification. ISOO should ensure that agencies pinpoint responsibility for determining need-to-know access.

COMMENT: Do not agree that ISOO should include a permanent inspection staff. ISOO's oversight function is to ascertain that agencies themselves are implementing an effective system of oversight.

ISOO and DIS are cooperating to develop improved instruction on information security and classification management.

Concur that the DCI should review special marking procedures, with the advice of the Director, ISOO.

Pinpointing agency responsibility for determining "need-to-know" access is simply not doable. It is everybody's business.

SECRET

SECRET

28. Postpone consideration of new criminal penalties for unauthorized disclosure until after the appeals in the Morison case. Continue internal agency and FBI investigations for purposes of administrative disciplines or prosecution, including use of voluntary polygraph examinations under criminal investigative procedures.

COMMENT: Concur with the second recommendation which mirrors current policy and procedures.

Non-concur, as a matter of principle, in the first recommendation while recognizing that action on legislative proposals to criminalize unauthorized disclosures will be influenced by ultimate disposition of the Morison case.

29. Review the Stilwell Commission proposals on managing and controlling classified information for government-wide implementation as part of the National Strategic Security Program.

COMMENT: This is being done by the IG/CM.

30. The Executive branch should determine the extent to which the FBI report to Congress

25X1

can be made public, and should advise the Committee. The report should be based on input from NSA and other appropriate agencies and should explain countermeasures already taken, underway, and planned.

25X1

COMMENT: Concur.

31. The National Strategic Security Program should ensure that NSA's plan for low-cost, secure voice telephone equipment includes all government agencies, contractors, and offices involved with national security information and other technological, political, and economic information of significant value to adversaries.

COMMENT: Concur in substance. NSDD-145 provides the structure for accomplishment of this planning. Implementation must be carefully prioritized and phased given the costs involved.

SECRET

SECRET

32. NSA should develop and submit to the Committee a plan, including resource requirements, for encryption of domestic commercial communications satellite links which are often the channels for private telephone messages vulnerable to interception, contrary to U.S. interests.

COMMENT: Concur in substance. Such planning is now under way pursuant to the responsibilities assigned to the National Manager for Telecommunications and Automated Information Systems Security. In accordance with NSDD-145, the plan focuses on satellite links which are often the channels for sensitive but unclassified information subject to unauthorized intercept and exploitation.

It is to be noted that several Congressional committees will need to review the plan and its resource requirements.

33. Joint FBI-DoD efforts to identify new clandestine technical threats to the security of communications, computers, and equipment in the United States should continue under the National Strategic Security Program.

COMMENT: Concur.

34. A first order of business for the National Strategic Security Program should be enforcement of current TEMPEST policy designed to relate expenditures more closely to the best counterintelligence estimates of actual and probable threats.

COMMENT: Concur.

35. The National Strategic Security Program should place greater emphasis on personnel and information security aspects of computer security, including research efforts, and should establish relative priorities for all aspects of computer security countermeasures.

COMMENT: Concur, noting that the physical security aspect also merits appropriate emphasis.

36. The computer security and information security communities should review and improve current procedures for analysis of information system

SECRET

SECRET

vulnerabilities before sensitive material is approved for storage in such systems.

COMMENT: Concur.

37. Given the gravity of the threat, high priority should be given to strict personnel security controls, comparable to the reinstituted crypto-access program and incorporating personnel reliability programs, for persons with extensive access or potential access to computer systems.

COMMENT: Agree that this is a key challenge and must be addressed. One should not underestimate the difficulty of determining the population to be included, establishing criteria, setting priorities, and developing management structure for such a program.

38. The National Strategic Security Program should provide for national-level review of communications, computer, and emanations security resource requirements, with NSA continuing to be responsible for development of technical measures needed to remedy vulnerabilities. The annual NSA budget justifications should be submitted to the Intelligence Committees for review.

COMMENT: Concur in substance, but question the relevance of the recommendation:

- NSDD-145 established structure for and mandated conduct of national-level review of resource requirements.
- In his capacity as National Manager for Telecommunications and Automated Information Systems Security, the Director, NSA has been assigned responsibility for conducting, approving, or endorsing R&D of techniques and equipment for telecommunications and automated information system security as well as reviewing and approving all standards, techniques, systems, and equipment for telecommunications and automated information systems.

The interest of the intelligence committees in the annual telecommunications and automated information systems security budget justification is understandable. It should be provided to them at the same time it is made available to the other cognizant committees for review.

SECRET

SECRET

39. The National Strategic Security Program should establish policies and priorities for technical surveillance countermeasures that take all interests and disciplines into account. In the near-term, CIA, NSA, and the State Department should reach agreement on an organizational framework and plan to be presented at a Committee hearing on security-related budget requests in April. In the long term, the National Strategic Security Program should include regular assessments of the technical surveillance threat in the United States and to U.S. interests abroad, as well as plans for government-wide security measures to counter the threat. The plans should address building construction needs and related personnel and information security requirements.

40. The State Department should implement vigorously a joint "tiger team" inspection system with CIA, NSA, and other agencies as necessary (such as FBI) having offensive as well as defensive expertise. The Technical Security Coordinating Group should provide mechanisms to bridge the offensive and defensive sides, safeguard sensitive capabilities, and recommend techniques for better defensive technical security operations. State should report to the Committee on the progress of the teams and its actions on their recommendations, as well as on the PTPE Center.

COMMENT: These two recommendations deal with a highly complex area. Understandably, then, #39 can be faulted for being too broad of scope and failing to delineate sharply between the short term (urgent and predominantly overseas), the longer term (domestic as well as overseas), and the interrelationship between the two. Moreover, #40 suggests that there may be some misunderstanding of the function of "Tiger Teams"--in reality, experts assembled to analyze specific vulnerabilities and recommend remedial action but no substitute for in-place security capabilities.

Consequently, it is suggested that the two recommendations be reformulated along the following lines.

SECRET

SECRET

"39. Greater emphasis must be placed on the development of means and the implementation of actions to detect and defeat increasingly sophisticated and aggressive efforts to effect technical penetration of sensitive facilities. Since US diplomatic missions abroad are now at serious threat, immediate priority must be accorded to measures to enhance their protection against technical attack. The ad hoc interagency group now functioning as a coordinating mechanism should be chartered to facilitate and expedite that effort. More specifically, this Technical Security Coordinating Group should provide mechanisms to bridge the offensive and defensive disciplines, to safeguard sensitive capabilities and operations; to develop methods and guidelines for improved technical security operations; and to address certain longer term issues, particularly the broad requirements and the identification of action offices responsible for incorporating security countermeasures designs into the Inman Supplemental construction programs. The Group should also develop principles and understandings, perhaps formalized by a jointly signed memorandum, regarding requirements to plan, activate, and deploy specialized expertise and equipments to overseas locations that may be vulnerable or subject to technical attacks. Such deployments will be tailored to specific objectives, coordinated and approved at appropriate levels and fully protected by tight operational security (OPSEC) procedures. State should report to the Committee on the progress of these cooperative efforts, including the [redacted]

25X1

25X1

"40. Concurrent with the foregoing, the technical surveillance countermeasures (TSCM) area should be reexamined in light of the longer term implications for sensitive facilities worldwide (domestic as well as overseas) of the technologically advanced Soviet capabilities and the vigor with which they are being applied. More focused attention on threat assessment, a stronger TSCM research base, and close interface with the Technical Security Coordinating Group are essential for sound planning. The organizational framework for interagency collaboration must facilitate the integration of technical security with other security disciplines."

41. The CIA should expand and upgrade its training school into a national center for TSCM with full NSA, State, military, and FBI participation and a greater role in fostering research, engineering, and operations. CIA should submit to the Committee a plan for this center, with provisions for training all Diplomatic Security Service and NSA personnel with TSCM duties

SECRET

SECRET

and for State and NSA to supply instruction, expert assistance, and information.

COMMENT: Concur.

42. The new Moscow embassy building should be certifiably "clean" before it is occupied. All agencies who will occupy the building must agree it is safe to do so.

COMMENT: Concur with the sense of the recommendation. It must be understood that "clean" will mean to the best of the ability of the experts and specifically including sufficient shielding and screening to provide confidence in the overall security of the embassy. Subsequent to occupation, it will be the responsibility of State to coordinate the implementation of the security countermeasures systems.

43. Congress and the Executive branch should support implementation of the Inman Panel recommendations for establishment of a Diplomatic Security Service and for major site and/or physical changes to U.S. facilities abroad to enhance security, minimize acts of terrorism, and deny hostile intelligence penetration.

COMMENT: Concur.

44. The National Strategic Security Program should foster better communication between U.S. counterintelligence agencies and industrial security officials to ensure that security officials are advised of indications of espionage by applicants and cleared personnel and to provide more tailored information on the hostile intelligence threats to particular programs or areas.

COMMENT: Concur. This is now being actively pursued.

45. DIS should initiate a pilot program for assignment of its personnel to large sensitive contractor facilities on a full-time basis, and the results should be reviewed as a basis for a similar government-wide practice.

COMMENT: Concur. DIS is in the process of developing a pilot program.

SECRET

SECRET

46. A two-year goal should be set for ending the reinvestigation backlog for contractors holding Top Secret and SCI clearances who are currently involved in sensitive classified contracts.

COMMENT: Do not concur. DoD, which has the great bulk of contractors, is now maintaining the SCI reinvestigation backlog at manageable levels. DoD has also established the goal of reducing the Top Secret reinvestigation backlog to manageable levels within four years. As a practical matter, DoD cannot treat the contractor component separately--nor does it see merit in so doing, were it practicable. This view is shared by DoE and CIA.

47. Greater efforts should be made to reduce the number of clearances held by industry. The DoD goal of a ten percent reduction in FY 1986 should be applied by the DCI (for SCI programs) and the Secretary of Energy.

COMMENT: Concur with sustained efforts to reduce clearances in industry to the minimum essential for effective performance. However, do not concur with the assignment of arbitrary reduction goals. The methods of achieving reductions are best left to the Secretaries of Defense and Energy and the DCI.

48. Federal Acquisition Regulations (FAR) should be changed to designate industrial security for classified contracts as a direct cost.

COMMENT: Support the intent of this recommendation; i.e., that security costs associated with particular contracts should be better identified and monitored. However, the proposal to so amend the FAR requires further analysis to determine whether it would, in fact, achieve the end sought (most effective security per dollar spent). One alternative would be to require security expenditures be itemized as part of a classified contract's overhead costs. Both should be examined to determine their likely effects before a decision is made as to the best approach. Regardless of how security costs associated with contracts are accounted for, the key issues are whether those funds are being spent prudently and applied solely against security requirements. This requires, inter alia, improved contract administration and audit procedures.

49. Consideration should be given to greater use of Cost Plus Award Fee contracts as an incentive for fulfilling contract security requirements.

SECRET

SECRET

COMMENT: No objection as phrased. The idea of rewarding contractors who fulfill security requirements in the most effective and economical manner is not new. There are, however, serious practical problems in implementing the concept in an equitable manner.

50. Government certification for all contractor security officers should be required for the award of each classified contract.

COMMENT: Non-concur as phrased. While the Harper report, Stilwell Commission, and earlier recommendations of the SSCI draft all stress training and certification of key security officers, rigid application of a pre-certification criterion would be counter-productive. Examples are (1) a company bidding for the first time on a classified contract, and (2) change of personnel in a given corporation. In these cases, the procedure is to expedite facility clearance and/or training during contract preliminaries and start-up.

51. The National Strategic Security Program should ensure implementation of the Stilwell Commission recommendations on National Disclosure Policy not only for military information, but for sensitive intelligence and nuclear matters as well.

COMMENT: The relevant Stilwell Commission recommendations have already been implemented. Application to other categories of information will be examined. It is worth noting that similar, but more stringent, rules already apply to national intelligence and cryptologic information.

52. Other Harper Committee recommendations approved by DoD should be implemented promptly and reviewed for government-wide adoption.

COMMENT: Concur. DoE and CIA, the only agencies, apart from DoD, that manage industrial security programs, are reviewing subject recommendations.